UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

MOHAMED OSMAN MOHAMUD,

Defendant.

Criminal Case No. 3:10-CR-00475-KI-1

OPINION AND ORDER

S. Amanda Marshall
United States Attorney
District of Oregon
Ethan D. Knight
Pamala R. Holsinger
United States Attorney's Office
1000 S.W. Third Avenue, Suite 600
Portland, Oregon 97204
John P. Carlin
George Z. Toscas
J. Bradford Wiegmann
Tashina Gauhar
Jolie F. Zimmerman

National Security Division
United States Department of Justice

Attorneys for Plaintiff

Steven T. Wax
Federal Public Defender
Stephen R. Sady
Lisa Hay
Office of the Federal Public Defender
101 SW Main Street, Suite 1700
Portland, Oregon 97204

Attorneys for Defendant

KING, Judge:

The Foreign Intelligence Surveillance Court of Review ("FISA Court of Review") has explained the difficult exercise which I now undertake:

> Our government is tasked with protecting an interest of utmost significance to the nation–the safety and security of its people. But the Constitution is the cornerstone of our freedoms, and government cannot unilaterally sacrifice constitutional rights on the altar of national security. Thus, in carrying out its national security mission, the government must simultaneously fulfill its constitutional responsibility to provide reasonable protections for the privacy of United States persons. The judiciary's duty is to hold that delicate balance steady and true.

In re Directives [Redacted] Pursuant to Section 105B of FISA, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008).

Title I and Title III of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. §§ 1801-1812, 1821-1829, allow electronic surveillance and physical search after obtaining a FISA warrant from the Foreign Intelligence Surveillance Court ("FISC"). The government provided a FISA notification to defendant at his first appearance, advising him it intended to use evidence

obtained under Title I and Title III. Defendant unsuccessfully relied on an entrapment defense. A jury convicted him in January 2013 of attempting to use a weapon of mass destruction, in violation of 18 U.S.C. § 2332a(a)(2)(A).

Section 702 of the FISA Amendments Act of 2008 ("FAA"), 50 U.S.C. § 1881a (part of Title VII of FISA, which is codified at §§ 1881a-1881g), permits, subject to statutory requirements, the targeting of non-United States persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information.

> Unlike traditional FISA surveillance, § 1881a does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power. And, unlike traditional FISA, § 1881a does not require the Government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur.
>
> . . . .
>
> Section 1881a mandates that the Government obtain the Foreign Intelligence Surveillance Court's approval of "targeting" procedures, "minimization" procedures, and a governmental certification regarding proposed surveillance.

Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1144-45 (2013) (internal citations omitted).

On November 19, 2013, the government filed a Supplemental FISA Notification:

> This supplemental notice is being filed as a result of the government's determination that information obtained or derived from Title I FISA collection may, in particular cases, also be "derived from" prior Title VII FISA collection. Based upon that determination and a recent review of the proceedings in this case, the United States hereby provides notice to this Court and the defense, pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), that the government has offered into evidence or otherwise used or disclosed in proceedings, including at trial, in the above-captioned matter information derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a.

Defendant intended to challenge the constitutionality of Title VII and claimed he needed broad discovery to provide the court with the full factual context surrounding the legal issues relevant to the newly-noticed surveillance. On March 19, 2014, I denied defendant's motion seeking this discovery. Now before the court are defendant's Motion for Vacation of Conviction and Alternative Remedies of Dismissal of the Indictment, Suppression of Evidence, and New Trial for the Government's Violation of the Pretrial Notice Statute [500], defendant's Alternative Motion for Suppression of Evidence and a New Trial Based on the Government's Introduction of Evidence at Trial and Other Uses of Information Derived from Unlawful Electronic Surveillance [502], and defendant's Second Motion for a New Trial [504]. Generally speaking, defendant seeks suppression of evidence obtained or derived through § 702 or fruits of that evidence, as well as other related or alternative relief. I deny the motions for the reasons I explain below. I am also filing an accompanying classified opinion to explain some of my reasoning.

DISCUSSION

I. Motion for Vacation of Conviction and Alternative Remedies of Dismissal of the Indictment, Suppression of Evidence, and New Trial for the Government's Violation of the Pretrial Notice Statute

Under 50 U.S.C. § 1881e(a), information acquired under § 702 is deemed information acquired from an electronic surveillance and is subject to the notice requirement in 50 U.S.C. § 1806(c). Defendant argues the government violated the notice statute by failing to provide notice of § 702 surveillance in the original pretrial FISA notification. As a remedy, defendant seeks dismissal of the indictment or a new trial after suppression of evidence.

Defendant first objects to what he contends are contradictory statements in the government's briefing for the discovery motion I just denied. Defendant sees a contradiction between: (1) the government's statement that it had not previously considered if evidence obtained through electronic surveillance under Title I/III could also be considered as a matter of law to be derived from a prior collection under Title VII and; (2) the government's statement that the prosecutors acted in accordance with the then-current standard practice.

The government explains it provided the Supplemental Notification after deciding evidence obtained under Title I/III could also be considered to be derived from prior collection under Title VII as a matter of law. A changed legal opinion is a different issue from following the standard practice up to that point. I do not see the contradiction troubling defendant.

Next, defendant claims he has established a prima facie case regarding the circumstances surrounding the statutory violation, relying on speculation and public disclosures about Clapper. He argues that to rebut this prima facie case, the government must file affidavits to support its explanation concerning the reason it filed the Supplemental Notification. This is not a situation, however, where the law supports presumptions based on a prima facie case.[1]

I now turn to the legal arguments defendant brings forward, the first of which is based on cases in effect when Congress enacted FISA. Because the FISA notice provision requires notice to both the aggrieved person and the court, defendant argues dismissal of the indictment or a new trial provide the only mechanisms to vindicate the separation of powers doctrine and to effectuate the choice the Supreme Court has imposed on the government. Defendant relies on a trilogy of Supreme

[1] I am unpersuaded the burden-shifting analysis for resolving summary judgment motions in employment discrimination cases, as set forth in McDonnell Douglas Corp. v. Green, 411 U.S. 792 (1981), and cited by defendant, has any application to the issue before me.

Court cases requiring the government to choose between disclosure and dismissal of the indictment: Jencks v. United States, 353 U.S. 657, 672, 77 S. Ct. 1007 (1957) (defendant was entitled to reports of government witnesses testifying at trial; the criminal action must be dismissed if the government, on the ground of privilege, elects not to comply with an order to produce), Roviaro v. United States, 353 U.S. 53, 61, 77 S. Ct. 623 (1957) (if an informer's identity is relevant and helpful to the defense or is essential to a fair trial, the government must disclose the identity or dismiss the indictment), and Alderman v. United States, 394 U.S. 165, 184, 89 S. Ct. 961 (1969) (in the context of electronic surveillance with no statutory notice requirement, government must disclose surveillance records needed to determine the legality of the surveillance or dismiss the indictment). Defendant contends these cases provide a framework for protection of the separation of powers because they enforce legislative and judicial constraints on executive over-reaching in prosecution.

The government's response is based on FISA's provision under 50 U.S.C. § 1806(e) which allows defendant to move to suppress evidence unlawfully acquired. Because this remedy would put defendant in a similar position to the government having provided the Supplemental Notification before trial, the government argues dismissal of the indictment is unnecessary. The government contends defendant's trilogy of Supreme Court cases do not apply to his situation because, here, the government did not affirmatively withhold disclosure of the use of the Title VII-derived evidence in defiance of a court order.

Congress was aware of Jencks, Roviaro, and Alderman when it enacted FISA, yet it chose to provide the single remedy of suppression, not dismissal of the indictment, when the government unlawfully acquired evidence under the statute. Defendant has argued no persuasive reason to limit the term "unlawfully acquired . . . under the statute" to exclude a failure to provide the statutory

notice. In addition, as the government notes, FISA even anticipates a suppression motion may be filed after trial: "Such a motion shall be made before the trial . . . unless . . . the person was not aware of the grounds of the motion." 50 U.S.C. § 1806(c). If Congress wished to provide a harsher penalty for a notification violation, it could have done so.

Alternatively, defendant claims the court can dismiss the indictment or grant a new trial to remedy the government's intentional or reckless violation of the FISA notice provision, based on an exercise of the court's inherent supervisory power, Federal Rule of Criminal Procedure 16(d), and Brady authority. Even if the government did not intentionally violate the notice provision, defendant claims the government's reckless disregard for the statutory obligation warrants dismissal.

The government argues dismissing the indictment would serve no valid purpose because there was no constitutional violation. Because FISA provides an appropriate remedy, the government contends defendant cannot show substantial prejudice, and the court may take less severe action than dismissal. The government claims there was no prosecutorial misconduct, much less flagrant misconduct, when it provided notice under the standard practice at the time. Once the government changed its legal opinion, it provided the Supplemental Notification which allowed defendant to file the pending motion to suppress. Further, the government argues there were no discovery violations and there is no new evidence, making sanctions under Rule 16 or Brady inappropriate.

I agree with defendant that I have the power to dismiss the indictment under my inherent supervisory powers and for violations of the discovery obligations under the Constitution and federal rules. See United States v. Chapman, 524 F.3d 1073, 1084-88 (9th Cir. 2008) (under its supervisory power, the court may dismiss an indictment for flagrant prosecutorial misconduct, which can include

reckless disregard for the prosecution's constitutional obligations under Brady and Giglio); United States v. Hernandez-Meza, 720 F.3d 760, 769 (9th Cir. 2013) (indictment can be dismissed for willful Rule 16 violation). But dismissal is not warranted here.

The court may exercise its supervisory power "to remedy a constitutional or statutory violation; to protect judicial integrity by ensuring that a conviction rests on appropriate considerations validly before a jury; or to deter future illegal conduct." United States v. Stinson, 647 F.3d 1196, 1210 (9th Cir. 2011) (internal quotations omitted), cert. denied, 132 S. Ct. 1768 (2012). Dismissal is available "when the investigatory or prosecutorial process has violated a federal constitutional or statutory right and no lesser remedial action is available." United States v. Barrera-Moreno, 951 F.2d 1089, 1092 (9th Cir. 1991).

As explained above, FISA provides a lesser remedy if necessary–suppression. Thus, the harsh remedy of dismissal is not needed. Clearly a lot of time has passed, but otherwise suppression and a new trial would put defendant in the same position he would have been in if the government notified him of the § 702 surveillance at the start of the case. Moreover, the government has apparently changed its practice in making this type of notification, so dismissal is not needed as a deterrence.

In addition, once the government changed its legal opinion about when evidence could be derived under Title VII, it performed the second review of this case and provided the Supplemental Notification without prodding from the court or the defense. If the government had kept mum about the situation in this case, I would have sentenced defendant months ago. I consider this strong evidence of the lack of prosecutorial misconduct.

For these reasons, I deny defendant's motion for vacation of conviction and alternative remedies of dismissal of the indictment, suppression of evidence, and new trial for the government's violation of the pretrial notice statute.

II. Second Motion for a New Trial

Defendant went to trial to present an entrapment defense. He argued he was not predisposed to attempt to use a weapon of mass destruction in the United States, and he was induced into doing so. He divides the withheld evidence into three parts: (1) the fact of additional surveillance; (2) the scope of that surveillance; and (3) the evidence generated by that surveillance. Defendant is at a grave disadvantage in articulating how the withheld evidence might have affected the trial, because he has not seen it, but he presents a few scenarios he considers likely.

According to defendant, if he had the withheld evidence before trial, he could have argued that the lack of evidence of predisposition, in light of the additional and pervasive surveillance, more strongly suggests he was not predisposed. With respect to inducement, defendant could have argued the knowledge the government gained through the additional surveillance allowed the government to more closely tailor the sting operation. Defendant claims the jury should have seen the withheld evidence to fully assess the government's conduct. Thus, defendant considers the late notification of the Title VII surveillance a Brady violation, as well as a violation of his other fundamental constitutional rights guaranteeing a fair trial, and he seeks a new trial as a remedy.

The government assumes defendant is moving for a new trial under Federal Rule of Criminal Procedure 33, which allows the court to grant a new trial if the interest of justice so requires or if there is newly discovered evidence. The government reminds us the Supplemental Notification referred to evidence previously addressed before trial that was derived from a Title VII collection as

well as being obtained in a Title I/III collection. Thus, the government argues there is no new evidence, and defendant's inference that the surveillance was pervasive in scope is only an inference, not new evidence. Moreover, the government claims the specific information at issue would not have been helpful to the defense or resulted in acquittal, as detailed in the government's classified brief. The government contends it presented overwhelming evidence of defendant's guilt at trial, and notes the jury convicted defendant even after the defense argued the pervasive scope of government surveillance to the jury.

Because defendant makes broad arguments, I will state a few standards which could apply. A party seeking a trial on newly discovered evidence must prove:

> (1) the evidence is newly discovered; (2) the defendant was diligent in seeking the evidence; (3) the evidence is material to the issues at trial; (4) the evidence is not (a) cumulative or (b) merely impeaching; and (5) the evidence indicates the defendant would probably be acquitted in a new trial.

United States v. Hinkson, 585 F.3d 1247, 1265 (9th Cir. 2009), reh'g denied and dissenting op. vacated and superseded, 611 F.3d 1098 (9th Cir. 2010).

For the court to grant a new trial because of a Brady violation, it must determine that the documents, if favorable to the defendant, "undermine its confidence in the outcome and that there is a reasonable probability of a different result." United States v. Doe, 705 F.3d 1134, 1152-53 (9th Cir. 2013) (internal quotation omitted).

Although defendant vehemently disagrees, the fundamental problem with defendant's argument is that there is no new evidence. A surveillance is not evidence–it produces evidence. Even with an entrapment defense, the way in which the government was able to tailor the sting operation is not relevant to entrapment. What is relevant to entrapment are the actual contacts

between government agents and the defendant. Those contacts were presented in detail to the jury, including hours of video and audio recordings. The jury was able to fully assess the government's conduct, as was I. The defense brought forward the pervasiveness of the surveillance of defendant, even lacking knowledge of the § 702 surveillance referenced in the Supplemental Notification. Moreover, even if there were a Brady violation, I cannot say my confidence in the outcome of the trial is undermined or that there is a reasonable probability of a different result.

Defendant further argues the government presented its investigation as being above reproach. He speculates that depending on the content of the withheld evidence, the defense might have been able to impeach government witnesses' characterizations of the investigation and thereby cast doubt on their credibility.

The government claims that even if the fact of the § 702 collection would impeach a government witness, new impeachment evidence does not support a motion for a new trial except in extraordinary circumstances.

As stated above in the factors for a new trial under Hinkson, impeachment evidence is usually not enough to support a request for a new trial. However, there is one exception:

> [T]he newly-discovered impeachment evidence may be so powerful that, if it were to be believed by the trier of fact, it could render the witness' testimony totally incredible. In such a case, if the witness' testimony were uncorroborated and provided the only evidence of an essential element of the government's case, the impeachment evidence would be "material" under [United States v. Walgren, 885 F.2d 1417, 1428 (9th Cir.1989)]. Moreover, Rule 33 permits the granting of a new trial motion "if required in the interest of justice." Fed. R. Crim. P. 33. If newly-discovered evidence establishes that a defendant in a narcotics case has been convicted solely on the uncorroborated testimony of a crooked cop involved in stealing drug money, the "interest of justice" would support a new trial under Rule 33.

United States v. Davis, 960 F.2d 820, 825 (9th Cir. 1991).

That is clearly not the situation here. Introduction of the fact of the § 702 surveillance referenced in the Supplemental Notification would not gut the government's case against defendant.

Accordingly, I deny defendant's second motion for a new trial.

III. Alternative Motion for Suppression of Evidence and a New Trial Based on the Government's Introduction of Evidence at Trial and Other Uses of Information Derived from Unlawful Electronic Surveillance

A. Overview of FISA

I first provide an overview of FISA's history and an explanation of some of its provisions:

As originally enacted in 1978, FISA generally requires a warrant to conduct electronic surveillance, as that term was defined in the Act. 50 U.S.C. § 1809(a)(1). Congress precisely defined electronic surveillance to cover four types of domestic foreign intelligence collection activities, with the type being dependent, in part, on whether a wire or a radio communication is being acquired. 50 U.S.C. § 1801(f). Based on witness testimony, Congress understood that most foreign-to-foreign and international communications were outside FISA's proposed definition of electronic surveillance.

> "[T]he language of this amendment exempts . . . foreign intelligence gathering from international or foreign communications by means of an electronic, mechanical, or other surveillance device if the acquisition does not come within the definition of "electronic surveillance" . . . . Specifically this provision is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States.

See S. Rep. No. 95-701, at 71 (1978).

According to the government, if a particular known U.S. person in the United States was not intentionally targeted, FISA, when first enacted, "allowed the government to monitor international

communications through radio surveillance, or wire surveillance of transoceanic cables offshore or on foreign soil, outside the statute's regulatory framework." Government's Unclassified Resp. to Def.'s Alternative Mot. for Suppression of Evidence and a New Trial 11, ECF No. 500 [hereinafter Govt.'s Brief]. Communications technology changed dramatically as the decades passed, causing unforeseen consequences under FISA.

> More specifically, the DNI [Director of National Intelligence] explained that, whereas international communications were predominantly carried by radio when FISA was enacted, that was no longer true: "Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally by fiber optic cables"–and therefore qualify as wire communications under FISA. [Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Select Comm. on Intel., 110th Cong. 1st Sess. (May 1, 2007), at 19. ("May 1, 2007 FISA Modernization Hrg.")] Thus, many international communications that would have been generally excluded from FISA regulation in 1978, when they were carried by radio, were now potentially included, due merely to a change in technology rather than any intentional decision by Congress. Id.
>
> Further, the DNI stated, with respect to the collection of wire communications, FISA's "electronic surveillance" definition "places a premium on the location of the collection." May 1, 2007 FISA Modernization Hrg. at 19; see 50 U.S.C. § 1801(f)(2). The DNI explained that technological advances had rendered this distinction outmoded as well: "Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a few miles apart." May 1, 2007 FISA Modernization Hrg. at 19.

Govt.'s Brief 13-14 (footnote omitted).

To update FISA, Congress enacted the Protect America Act ("PAA") in August 2007; under a sunset provision, it expired in February 2008. In July 2008, Congress enacted the FISA Amendments Act of 2008 ("FAA"), including § 702, the center of the dispute in this motion. Under § 702, after the FISC issues an order, the Attorney General and the DNI "may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably

believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a).

Section 702 includes limitations to protect domestic communications. An acquisition:

> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
>
> (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
>
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
>
> (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
>
> (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

50 U.S.C. § 1881a(b).

Minimization procedures "are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1).

If the FISC approves the targeting and minimization procedures and the certification from the Attorney General and DNI, it will approve the acquisition. Under 50 U.S.C. § 1881a(g)(2)(A), the certification must attest:

(1) there are procedures in place that have been approved, submitted for approval, or will be submitted with the certification for approval by the FISC that are reasonably designed to ensure that an acquisition (a) is limited to targeting persons reasonably believed to be located outside the United States and (b) to prevent the intentional acquisition of any communication in which the sender and all intended recipients are known to be located in the United States;

(2) the minimization procedures meet the definition of minimization procedures under Title I/III and have been approved, submitted for approval, or will be submitted with the certification for approval by the FISC;

(3) the Attorney General has adopted guidelines to ensure compliance with the limitations in 50 U.S.C. § 1881a(b) [quoted above];

(4) the procedures and guidelines are consistent with the requirements of the Fourth Amendment;

(5) a significant purpose of the acquisition is to obtain foreign intelligence information;

(6) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

(7) the acquisition complies with the limitations in 50 U.S.C. § 1881a(b) [quoted above];

In addition, the certification must include copies of the targeting and minimization procedures, a supporting affidavit from an appropriate national security official, and an effective date. 50 U.S.C. § 1881a(g)(2)(B)-(D). The FISC can approve the certification and related targeting and minimization procedures, or it can direct the government to either (1) correct any deficiency within 30 days or (2) cease or not begin implementation of the authorization. 50 U.S.C. § 1881a(i)(3)(B).

Section 702 allows the government to compel an electronic communication service provider to acquire the authorized communications. 50 U.S.C. § 1881a(h). The National Security Agency ("NSA") "provides specific identifiers (for example, e-mail addresses, telephone numbers) used by non-U.S. persons overseas who the government believes possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification." The National Security Agency: Missions, Authorities, Oversight and Partnerships 4, available at http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf (Aug. 9, 2013).

B. Separation of Powers

As a threshold issue, defendant claims § 702 violates the separation of powers doctrine. The Fourth Amendment inserts a neutral and detached magistrate between the subject of the search and the government. Defendant claims § 702 procedures reduce the role of the judge to consulting with the Executive Branch with no case or controversy involving an adversary. He contends the FISC does not approve or disapprove proposals for § 702 surveillance but instead has a role in designing them. Defendant characterizes the FISC's role as providing a non-judicial advisory opinion, and he argues this violates the fundamental separation of powers function of the Warrant Clause.

The government disagrees and analogizes the FISC role to numerous judicial functions not directly connected to adversarial proceedings.

The FISA Court of Review has noted it does "not think there is much left to an argument made by an opponent of FISA in 1978 that the statutory responsibilities of the FISA court are inconsistent with Article III case and controversy responsibilities of federal judges because of the secret, non-adversary process." In re Sealed Case, 310 F.3d 717, 732 n.19 (FISA Ct. Rev. 2002)

(citing Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, 9745, 7308, and 5632 Before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence, 95th Cong., 2d Sess. 221 (1978) (statement of Laurence H. Silberman)). I agree.

The Supreme Court has approved numerous congressional delegations of power which did not upset the balance of power established in the Constitution:

> The nondelegation doctrine is rooted in the principle of separation of powers that underlies our tripartite system of Government. The Constitution provides that "[a]ll legislative Powers herein granted shall be vested in a Congress of the United States," U.S. Const., Art. I, § 1, and we long have insisted that "the integrity and maintenance of the system of government ordained by the Constitution" mandate that Congress generally cannot delegate its legislative power to another Branch. Field v. Clark, 143 U.S. 649, 692, 12 S. Ct. 495, 504, 36 L. Ed. 294 (1892). We also have recognized, however, that the separation-of-powers principle, and the nondelegation doctrine in particular, do not prevent Congress from obtaining the assistance of its coordinate Branches. . . . So long as Congress "shall lay down by legislative act an intelligible principle to which the person or body authorized to [exercise the delegated authority] is directed to conform, such legislative action is not a forbidden delegation of legislative power." J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394, 409, 48 S. Ct. 348, 352 (1928).

Mistretta v. United States, 488 U.S. 361, 371-72, 109 S. Ct. 647 (1989) (holding Sentencing Guidelines are constitutional, Congress did not delegate excessive legislative power to the Commission and did not violate the separation-of-powers principle, judges traditionally determine sentences). "[C]onsistent with the separation of powers, Congress may delegate to the Judicial Branch nonadjudicatory functions that do not trench upon the prerogatives of another Branch and that are appropriate to the central mission of the Judiciary." Id. at 388.

The statutory scheme Congress specified for § 702 surveillance is sufficient to serve as the intelligible principle to which FISC judges must conform in reviewing applications. In particular, the FISC review must insure the surveillance will be conducted in a manner consistent with the

Fourth Amendment. 50 U.S.C. § 1881a(b)(5), (g)(2)(A)(4). The judiciary certainly is well-prepared to fulfill that function. Furthermore, determining if a statute is constitutional is not a prohibited executive or administrative duty which would violate the separation of powers doctrine. See Morrison v. Olson, 487 U.S. 654, 677, 108 S. Ct. 2597 (1988) (in upholding the constitutionality of the Ethics and Government Act under Article III and the separation of powers doctrine, the Court noted, "As a general rule, we have broadly stated that executive or administrative duties of a nonjudicial nature may not be imposed on judges holding office under Art. III of the Constitution.") (internal quotation omitted).

Indeed, as the government points out, the judiciary also issues search warrants and reviews wiretap applications, both of which are ex parte proceedings. Id. at 389 n.16. I am not persuaded the review of § 702 surveillance applications interferes with the prerogatives of another branch of government beyond requiring the executive branch to conform to the statute. Review of § 702 surveillance applications is as central to the mission of the judiciary as the review of search warrants and wiretap applications.

Moreover, I disagree with defendant's argument that the FISC judges only provide advisory opinions. The FISC judge reviews the certification, targeting procedures, and minimization procedures included in a § 702 surveillance application and either approves the acquisition or orders the government to choose between correcting deficiencies within 30 days and ceasing or not beginning the acquisition. 50 U.S.C. § 1881a(i)(2). Similarly, electronic communication service providers must follow directives to acquire communications or challenge the directive before the FISC; the opinions are not advisory. 50 U.S.C. § 1881a(h).

Although I am not a FISC judge, I disagree with defendant's argument that the FISC judges assist in designing § 702 procedures. FISC opinions now declassified inform us that the court meets with senior officials at the Department of Justice to discuss information provided in the submissions. [Caption Redacted], [docket no. redacted], 2011 WL 10945618, at *3 (FISA Ct. Oct. 3, 2011). The technology underlying the surveillance is so extremely complex there is likely little possibility of understanding it without question sessions like this. If the FISC disapproves a government submission, it explains why. The government can then make changes addressing the problems and resubmit the submission. This is the normal way courts operate–justice is not served if the court does not explain its decisions.

Finally, "[p]rior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights." United States v. United States Dist. Court for E. Dist. of Mich., 407 U.S. 297, 318, 92 S. Ct. 2125 (1972)(citing Beck v. Ohio, 379 U.S. 89, 96, 85 S. Ct. 223 (1964)) (in the criminal prosecution for the bombing of a CIA office in Michigan, warrantless wiretaps conducted as part of a domestic security surveillance violated the Fourth Amendment) [hereinafter Keith]. Although the FISC is not reviewing a warrant application under § 702, the FISC review of § 702 surveillance submissions provides prior review by a neutral and detached magistrate. This strengthens, not undermines, Fourth Amendment rights.

Accordingly, I conclude § 702 does not violate the separation of powers doctrine.

C. Constitutionality of Section 702 under the First Amendment

Defendant contends the breadth and vagueness of § 702 surveillance chill Americans' exercise of their First Amendment rights, causing many to change their habits in using the Internet

and telephones. Defendant claims this chill is sufficient to create a First Amendment violation, invalidating § 702.

The government responds that First Amendment interests in a criminal investigation are protected by the Fourth Amendment, and motions to suppress based on alleged First Amendment violations are analyzed under the Fourth Amendment and the exclusionary rule.

Defendant raises a significant point: "Where the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with scrupulous exactitude." Zurcher v. Stanford Daily, 436 U.S. 547, 564, 98 S. Ct. 1970 (1978) (internal quotation omitted) (a search warrant for a newspaper which was not suspected of a crime does not violate the First Amendment because the warrant's preconditions adequately safeguard the newspaper's ability to gather and publish the news).

But the appropriate analysis is under the Fourth Amendment, not the First Amendment. United States v. Mayer, 503 F.3d 740, 747-48 (9th Cir. 2007) (affirming conviction based on investigation with FBI agent going undercover as a member of organization opposed to sexual age-of-consent laws, "First Amendment concerns become part of the Fourth Amendment analysis because, under the Fourth Amendment, the court must examine what is unreasonable in the light of the values of freedom of expression" (citing Roaden v. Kentucky, 413 U.S. 496, 504, 93 S. Ct. 2796 (1973))).

Defendant cites a concurrence in Nevada Commission on Ethics v. Carrigan for the proposition that a statute is invalid if it "operates to chill or suppress the exercise of First Amendment freedoms by reason of vague terms or overbroad coverage." Nevada Commission on Ethics v. Carrigan, 131 S. Ct. 2343, 2353 (2011) (Kennedy, J., concurring) (state government

conflict of interest rule did not violate legislator's First Amendment rights). I have no quarrel with this blackletter statement of the law, but Nevada Commission on Ethics is far afield from § 702 surveillance.

Consequently, I will follow Mayer and move on to a Fourth Amendment analysis, but I will apply the Fourth Amendment requirements with "scrupulous exactitude," as required by Zurcher.

D. Constitutionality of Section 702 under the Fourth Amendment

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

"[N]either a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance." Nat'l Treasury Emp. Union v. Von Raab, 489 U.S. 656, 665, 109 S. Ct. 1384 (1989) (suspicionless drug-testing of certain United States Custom Service employees was reasonable under Fourth Amendment).

The parties agree on one thing: The Fourth Amendment does not "apply to activities of the United States directed against aliens in foreign territory." United States v. Verdugo-Urquidez, 494 U.S. 259, 267, 110 S. Ct. 1056 (1990) (Fourth Amendment did not apply to American law enforcement's search of the Mexican residences of a Mexican citizen with no voluntary attachment to the United States). Section 702 is aimed at acquiring communications of non-U.S. persons outside the United States, and thus not entitled to Fourth Amendment protection. The dispute arises because communications of U.S. persons located in the United States can be incidentally acquired.

The government claims the § 702 acquisition targeting non-U.S. persons outside the United States is constitutional because: (1) the incidental collection of communications of U.S. persons does not trigger the warrant requirement; (2) surveillance authorized under § 702 falls within the foreign intelligence exception to the warrant requirement; and (3) surveillance authorized under § 702 is a reasonable search under the Fourth Amendment.

Defendant strongly disagrees:

> [R]egardless of the nominal targeting of foreign persons abroad, the § 702 programs routinely acquire huge numbers of American communications in America . . . [which] implicate[] the Fourth Amendment. This case is a test of fundamental American liberties: the Court should reject the claim that, simply because foreign persons are being targeted, Americans lose their rights as collateral damage.

Def.'s Reply to Government's Unclassified Resp. to Def.'s Alternative Mot. for Suppression of Evidence 4, ECF No. 513 [hereinafter Def.'s Reply].

First, I must address whether defendant's challenge to § 702 must be limited to an "as applied" challenge, as the government argues, or also include a facial challenge, as defendant argues. Defendant relies on Berger v. State of New York, 388 U.S. 41, 87 S. Ct. 1873 (1967), in which the Court held a state statute, allowing law enforcement to obtain ex parte orders for eavesdropping, violated the Fourth Amendment because it was overbroad and allowed "a trespassory invasion of the home or office, by general warrant." Id. at 44, 64. The Court allowed the facial challenge, even though the defendant was convicted using evidence obtained by the eavesdropping order. Id. at 44. The Court took the opposite approach in Sibron v. New York, 392 U.S. 40, 59, 88 S. Ct. 1889 (1968) (refusing to undertake a facial challenge to the constitutionality of New York's stop-and-frisk law), and distinguished Berger:

> The parties on both sides of these two cases have urged that the principal issue before us is the constitutionality of § 180-a 'on its face.' We decline, however, to be drawn into what we view as the abstract and unproductive exercise of laying the extraordinarily elastic categories of § 180-a next to the categories of the Fourth Amendment in an effort to determine whether the two are in some sense compatible. The constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case. In this respect it is quite different from the question of the adequacy of the procedural safeguards written into a statute which purports to authorize the issuance of search warrants in certain circumstances. See [Berger]. No search required to be made under a warrant is valid if the procedure for the issuance of the warrant is inadequate to ensure the sort of neutral contemplation by a magistrate of the grounds for the search and its proposed scope, which lies at the heart of the Fourth Amendment.

Sibron, 392 U.S. at 59 (internal citation omitted).

Defendant contends his facial challenge to § 702 concerns the adequacy of its procedural safeguards, and should be allowed under Berger.

The government insists the challenge must be limited to "as applied," citing In re Directives, 551 F.3d at 1010, which limited the communication service provider's challenge to "as applied." Specifically, "[w]here, as here, a statute has been implemented in a defined context, an inquiring court may only consider the statute's constitutionality in that context; the court may not speculate about the validity of the law as it might be applied in different ways or on different facts." In turn, In re Directives cited National Endowment for the Arts v. Finley, 524 U.S. 569, 118 S. Ct. 2168 (1998), in which the Court concluded a statute setting some guidelines in awarding financial grants for the arts did not violate the First Amendment. Although the plaintiffs had been denied a grant, the Court held the statute was *facially valid* "as it neither inherently interferes with First Amendment rights nor violates constitutional vagueness principles." Id. at 573. In doing so, the Court reasoned:

> Facial invalidation "is, manifestly, strong medicine" that "has been employed by the Court sparingly and only as a last resort." Broadrick v. Oklahoma, 413 U.S.

> 601, 613, 93 S. Ct. 2908, 2916, 37 L. Ed. 2d 830 (1973); see also FW/PBS, Inc. v. Dallas, 493 U.S. 215, 223, 110 S. Ct. 596, 603, 107 L. Ed. 2d 603 (1990) (noting that "facial challenges to legislation are generally disfavored"). To prevail, respondents must demonstrate a substantial risk that application of the provision will lead to the suppression of speech.

Id. at 580.

The Court also noted it was "reluctant, in any event, to invalidate legislation on the basis of its hypothetical application to situations not before the Court." Id. at 574 (internal quotation omitted).

If I use defendant's proffered standard in a facial challenge, that there would be a substantial risk the statute would be applied unconstitutionally, rather than the government's proffered standard, that the statute would survive a facial challenge if there is any set of circumstances in which it could be constitutionally applied,[2] I would be required to speculate about the other applications. Under the government's standard, if the statute survives an as-applied challenge, it automatically survives a facial challenge because there is at least one constitutional application. I am unwilling to speculate on other applications with a statute this complex. Moreover, although defendant argues I should undertake a facial challenge to address the lack of procedural safeguards in § 702, the allegedly insufficient procedural safeguards were applied to defendant, so I would address them in an as-applied challenge also. This includes the lack of a warrant, the lack of any probable cause determination, and the lack of any judicial determination about a targeted individual, due to the programmatic nature of § 702 surveillance. This overlap, as well as the complexity, weigh in favor of an as-applied challenge.

---

[2] Based on United States v. Salerno, 481 U.S. 739, 745, 107 S. Ct. 2095 (1987).

For these reasons, I will follow the lead of the FISA Court of Review in In re Directives and limit defendant's challenge to an as-applied challenge.

1. Warrant Requirement

Defendant, a U.S. citizen, was not targeted under § 702, but his communications were collected incidentally during intelligence collection targeted at one or more non-U.S. persons outside the United States.

The government contends the warrant requirement is not triggered by the incidental collection of non-targeted U.S. person communications during the lawful collection of communications of targeted non-U.S. persons located outside the United States. According to the government, the privacy interests of the U.S. persons are protected by the required minimization procedures. Application of a warrant requirement in this situation would be impracticable and inconsistent with decades of foreign-intelligence collection practice. The government notes that before starting surveillance of a foreign target, the government cannot know the identities of all people with whom the target will communicate, and there is always a possibility the target will communicate with a U.S. person. Thus, the government claims imposing a warrant requirement for any incidental interception of U.S. person communications would effectively require a warrant for all foreign intelligence collection, even though the foreign targets lack Fourth Amendment rights and their communications often involve only other foreigners. Testimony before Congress supports the government's argument. See Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II) Hearing Before the H. Comm. on the Judiciary, 110th Cong., 1st Sess. at 8 (Sept. 18, 2007) (statement of

Rep. Forbes) ("would reverse 30 years of established intelligence gathering" and deprive the intelligence community of the flexibility needed to protect the country).

Defendant argues § 702 violates the Fourth Amendment because it permits the "widespread capture, retention, and later querying, dissemination, and use of the communications of American citizens" without the protection afforded by a warrant. Def.'s Mem. in Supp. of Alternative Mot. for Suppression of Evidence 13, ECF No. 503 [hereinafter Def.'s Brief]. Defendant notes the FISC's statement that the NSA acquires more than 250 million Internet communications each year under § 702, including acquisitions from upstream and from Internet service providers. [Caption Redacted], 2011 WL 10945618, at *9. Defendant speculates that a significant number of those acquisitions would be communications with U.S. persons located in the United States and thus implicate their Fourth Amendment rights sufficiently that the court should apply a warrant requirement.

The government cites cases supporting its argument that applying a warrant requirement to incidental interception of U.S.-person communications during surveillance targeting non-U.S. persons overseas to obtain foreign intelligence is inconsistent with decades of foreign intelligence collection practice. See In re Terrorist Bombings of United States Embassies in East Africa, 552 F.3d 157, 167 (2nd Cir. 2008) (Fourth Amendment's reasonableness requirement, not the Warrant Clause, governs extraterritorial searches of U.S. citizen's home and telephone); United States v. Barona, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995) (foreign searches historically have not been subject to the warrant procedure).

In addition, "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful." In re Directives, 551 F.3d at 1015 (in the

context of the PAA). The § 702 acquisition targeting a non-U.S. person overseas is constitutionally permissible, so, under the general rule, the incidental collection of defendant's communications with the extraterritorial target would be lawful. The one distinguishing factor is the possible vast number of incidental communications collected under § 702. I stress the word "possible." It is equally likely that § 702 surveillance of a non-U.S. person located outside the United States would acquire no incidental communications with a U.S. person. Consequently, I am unpersuaded incidental communications collected under § 702 differ sufficiently from previous foreign intelligence gathering to distinguish prior case law, and I hold that § 702 surveillance does not trigger the Warrant Clause.

Alternatively, as I explain in the next section, even if § 702 surveillance triggers the Warrant Clause, no warrant is required because § 702 surveillance falls within the foreign intelligence exception to the warrant requirement.

2. Foreign Intelligence Exception

Assuming the incidental collection of U.S.-person communications under § 702 is subject to the same constitutional scrutiny as foreign intelligence collection targeting U.S. persons, the government contends the Fourth Amendment does not require a warrant for § 702 surveillance because it falls within the foreign intelligence exception.

The Fourth Amendment's warrant requirement applies to domestic national security surveillance. Keith, 407 U.S. at 320. Defendant argues that even if there is a foreign national security exception to the Warrant Clause, the exception's scope is far narrower than the massive surveillance programs under § 702. Defendant claims the reasoning in Keith applies equally well to foreign national security surveillance, especially because of the First Amendment implications in the

seizure of phone calls and emails. Citing several cases, defendant argues "[p]rogrammatic intrusions into privacy generally involve openly implemented safety programs that must be carefully confined to a 'primary purpose' other than law enforcement to guard against abuse." Def.'s Reply 13. See Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 115 S. Ct. 2386 (1995) (program requiring random urinalysis of school athletes to test for drug use, with the purpose of deterring drug use, was constitutional). Because § 702 requires obtaining foreign intelligence to be a *significant* purpose of an acquisition, not a *primary* purpose, defendant argues the bleed-over into criminal investigations is especially high and contends the special needs doctrine should not apply. Defendant is alarmed that the statutory definition of foreign intelligence information in 50 U.S.C. § 1801(e) includes information unrelated to any danger to the country. He also argues that even if the special needs doctrine covers the acquisition of the information, it should not also cover the retention and later querying of the information.

The government disagrees, arguing the special needs exceptions to the Warrant Clause include a foreign intelligence exception. The government cites numerous cases to support its argument and notes that, with the exception of In re Directives, the cases involved the collection of foreign intelligence information from persons *inside* the United States. Because § 702 targets non-U.S. persons reasonably believed to be *outside* the United States, the government contends the analysis in its cases applies even more strongly. The government agrees the amount of intrusiveness and executive discretion are relevant to the reasonableness of a government program designed to serve a special need, but claims those factors do not decide whether the doctrine applies as an exception to the Warrant Clause.

Under this doctrine, the Court has approved exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, makes the warrant and probable-cause requirement impracticable." Griffin v. Wisconsin, 483 U.S. 868, 873, 107 S. Ct. 3164 (1987) (internal quotation omitted). In those situations, the Court "employed a balancing test that weighed the intrusion on the individual's interest in privacy against the 'special needs' that supported the program." Ferguson v. City of Charleston, 532 U.S. 67, 78, 121 S. Ct. 1281 (2001) (special needs doctrine did not apply; Fourth Amendment violated by hospital's performance of urine tests on patients to provide law enforcement evidence of criminal drug use). The Court has approved warrantless searches under the special needs doctrine in various circumstances. See Griffin, 484 U.S. 868 (warrantless searches of probationers' homes to look for contraband); Vernonia, 515 U.S. 646 (school's warrantless drug tests of athletes to deter drug use); Von Raab, 489 U.S. 656 (warrantless drug testing of employees seeking promotion to positions that directly involve the interdiction of illegal drugs or that require the employee to carry a firearm).

Several courts have analyzed and applied the foreign intelligence exception:

> After Keith, several courts of appeals, including our own, have examined the Fourth Amendment's application to electronic surveillance conducted under the guise of the President's executive authority to collect foreign intelligence information. These courts almost uniformly have concluded that the important national interest in foreign intelligence gathering justifies electronic surveillance without prior judicial review, creating a sort of "foreign intelligence exception" to the Fourth Amendment's warrant requirement. See, e.g., United States v. Truong Dinh Hung, 629 F.2d 908, 914 (4th Cir. 1980) ("[B]ecause of the need of the executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance."); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (en banc) (holding, in light of the "strong public interest" in uninterrupted foreign intelligence collection, that the Fourth Amendment does not require "prior judicial authorization" of surveillance "conducted and maintained solely for the purpose of gathering foreign

> intelligence information"). See generally [United States v. Duggan, 743 F.2d 59, 72 (2d Cir. 1984)] (summarizing foreign intelligence exception cases).

United States v. Duka, 671 F.3d 329, 341 (3rd Cir. 2011) (in analyzing convictions obtained pursuant to a traditional FISA warrant, holding FISA's amended "significant purpose" requirement is reasonable under the Fourth Amendment).

Notably, the FISA Court of Review applied a foreign intelligence exception "when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States." In re Directives, 551 F.3d at 1012 (requiring a communications service provider to comply with a directive to assist in warrantless surveillance under the PAA). The court reasoned: (1) the purpose of the surveillance went well beyond any "garden-variety" law enforcement objective and involved the acquisition from overseas foreign agents of foreign intelligence to help protect national security; (2) the government's interest was "particularly intense"; and (3) there was a "high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." Id. at 1011-12.

Precisely on point with the case before me, the FISC held that the foreign intelligence exception also applies to § 702 surveillance, even though the court's understanding of the technical situation underlying the surveillance changed after the government released more information:

> The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the "foreign intelligence exception" to the warrant requirement of the Fourth Amendment. See Docket No. [redacted]. The government's recent revelations regarding NSA's acquisition of MCTs [multi-communication transactions] do not alter that conclusion. To be sure, the Court now understands that, as a result of the transactional nature of the upstream collection,

> NSA acquires a substantially larger number of communications of or concerning United States persons and persons inside the United States than previously understood. Nevertheless, the collection as a whole is still directed at [redacted] conducted for the purpose of national security–a purpose going "'well beyond any garden-variety law enforcement objective.'" Further, it remains true that the collection is undertaken in circumstances in which there is a "'high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.'" Id. at 36 (quoting In re Directives at 18). Accordingly, the government's revelation that NSA acquires MCTs as part of its Section 702 upstream collection does not disturb the Court's prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA's targeting and minimization procedures.

[Caption Redacted], 2011 WL 10945618, at *24 (citation omitted) (granting in part and denying in part the government's requests for approval of § 702 certifications and procedures; one aspect of the proposed upstream collection of Internet transactions containing MCTs is not reasonable under the Fourth Amendment).

None of defendant's arguments persuade me to stray from the FISC's holding. I realize § 702 requires the significant purpose, not the primary purpose, of the acquisition be to obtain foreign intelligence information. 50 U.S.C. § 1881a(g)(2)(A)(5). The cases discussing the special needs doctrine do not use the phrase "primary purpose" as a term of art, and many do not even use it at all. See, e.g., Vernonia, 515 U.S. 646. There is no reasonable argument the government's need for the acquisitions is merely routine law enforcement. The government's need for speed and stealth have not lessened since the FISC decided [Caption Redacted], which found that application of the warrant requirement would be impracticable. When I balance the intrusion on the individual's interest in privacy, namely the incidental collection of U.S. persons' communications, against these special needs when the government targets a non-U.S. person believed to be outside the United States, I conclude the foreign intelligence exception applies and no warrant is required.

I will address defendant's concerns about the dual nature of the statutory definition of foreign intelligence information, 50 U.S.C. § 1801(e), in the next section analyzing the reasonableness of the acquisitions.

3. Reasonableness

Application of the foreign intelligence exception does not end the analysis: "even though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement." In re Directives, 551 F.3d at 1012.

To analyze whether a government search is reasonable under the Fourth Amendment, the court examines the totality of the circumstances. Samson v. California, 547 U.S. 843, 848, 126 S. Ct. 2193 (2006). The court weighs "'the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy." Maryland v. King, 133 S. Ct. 1958, 1970 (2013) (internal quotation omitted) (search using buccal swab inside the cheek to obtain DNA sample after arrest for serious offense is a legitimate police booking procedure that is reasonable under Fourth Amendment).

a. General Contentions

Defendant claims § 702 is presumptively unreasonable because it does not require a warrant, even though the acquired telephone calls and emails are within the core zone of privacy protected from government intrusion. See United States v. Katz, 389 U.S. 347, 353, 88 S. Ct. 507 (1967) (FBI agents' use of an electronic listening device attached to the outside of a phone booth to hear one side of a telephone conversation constituted a search and seizure under the Fourth Amendment); United

States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (warrant requirement applied to emails sent through a commercial internet service provider).

Defendant claims the Warrant Clause is the key metric in determining reasonableness. He disputes that the programmatic authorizations and certifications from the FISC under Title VII offer the protections traditional warrants afford. Defendant lists several protections provided under the Warrant Clause which are missing from § 702 surveillance:

> a) a warrant authorizing the search and seizure; b) based upon probable cause; c) particularly describing the place to be searched and the items to be seized; d) based on an affidavit under oath or affirmation; e) issued by a neutral and detached magistrate operating in a judicial capacity; f) with a return or other procedure assuring compliance with the terms of the warrant in its execution.

Def.'s Brief 17-18.

Because § 702 lacks these protections, defendant contends its use is either presumptively unreasonable or, alternatively, the extreme disconnect between § 702 procedures and basic Fourth Amendment warrant protections shows the unreasonableness of searches and seizures under § 702. Even though the FISC approves general programs and procedures under § 702, defendant argues the FISC does not review the government's specific targeting decisions or its later access of seized communications. Defendant contends the government should not be allowed to read the contents of American citizens' electronic communications without a judicial finding of probable cause. Further, defendant argues the government interest in acquiring "foreign intelligence information" is unreasonable under the Fourth Amendment because the term is so broadly defined under 50 U.S.C. § 1801(e), it goes well beyond threats to national security.

According to the government, surveillance under § 702 satisfies the Fourth Amendment's general reasonableness test. It claims the significant interest in national security, in light of FISA's

statutory safeguards, outweigh the privacy interests of U.S. persons whose communications are incidentally acquired. The government suggests U.S. persons have limited expectations of privacy in electronic communications with non-U.S. persons outside the United States.

The government relies heavily on In re Directives, in which the FISA Court of Review held the PAA, a statute which expired in 2008, was reasonable under the Fourth Amendment. Defendant notes the differences between § 702 and the PAA to argue it is not persuasive when analyzing § 702. First, programs under the PAA did not involve retaining a database of incidentally collected information from non-targeted U.S. persons which could be queried later. In re Directives, 551 F.3d at 1015. Second, because the PAA incorporated § 2.5 of Executive Order 12333, it required an executive determination of probable cause to believe the technique was directed against a foreign power or an agent of a foreign power. Id. at 1014.

I note, importantly, the PAA allowed the government to conduct warrantless foreign intelligence surveillance on targets reasonably believed to be located outside the United States, *including* U.S. persons. In re Directives, 551 F.3d at 1006. Section 702 prohibits targeting U.S. persons, even if they are outside the United States. 50 U.S.C. § 1881a(b)(3). In this respect, the PAA allowed much broader surveillance than § 702 does. I consider this difference significant and believe the analysis in In re Directives is particularly instructive.

b. Comparison of Section 702 to Protections Afforded by a Warrant

I will first address defendant's arguments comparing the protections provided by a warrant to those provided under § 702.

The Fourth Amendment states, in part: "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

In specifically addressing arguments about prior judicial review, probable cause, and particularity, the FISA Court of Review refused to "reincorporate into the foreign intelligence exception the same warrant requirements that we already have held inapplicable." In re Directives, 551 F.3d at 1013. The court explained, "the more a set of procedures resembles those associated with the traditional warrant requirements, the more easily it can be determined that those procedures are within constitutional bounds." Id. With this guidance in mind, I turn to the arguments.

Without the protections of the particularity requirement, defendant contends the communications of American citizens are swept up by § 702 surveillance in a dragnet fashion prohibited by the Fourth Amendment. Defendant also contrasts the Warrant Clause's requirement of a supporting affidavit under oath with the § 702 procedures for authorization. Defendant is concerned the § 702 procedures fall far short of the oath or affirmation provision of the Warrant Clause, particularly because the certification does not deal with particular persons or events.

The government notes the Attorney General and DNI must certify that targeting and minimization procedures are in place which are consistent with the Fourth Amendment and that a significant purpose of the acquisition is to obtain foreign intelligence information. The government contends the certification requirement represents an important internal check on the actions of the Executive Branch. It claims defendant's argument, that the government may target entire geographical areas or groups of people or read every American communication with a country of interest, is an accusation the government will not abide by the required procedures, despite extensive

oversight. To the contrary, the government argues the targeting procedures determine that "the user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States." [Caption Redacted], 2011 WL 10945618, at *7.

The lack of an oath requirement in § 702, as well as any argument the government will not follow the law, is unpersuasive. Absent evidence of fraud or misconduct, a presumption of regularity attaches to obtaining a warrant. The FISA Court of Review applied the same presumption to the government's procurement of a directive to a communications service provider under the PAA. In re Directives, 551 F.3d at 1014-15. I have seen no evidence of government fraud or misconduct in this case, and the differences between the PAA and § 702 do not weigh against applying the same presumption of regularity here.

Turning to the particularity requirement, § 702 surveillance uses targeting and minimization procedures approved by the FISC. [Caption Redacted], 2011 WL 10945618, at *6 ("The Court found in those prior dockets that the targeting and minimization procedures [as applied to forms of to/from communications that have previously been described to the Court] were consistent with the requirements of 50 U.S.C.§ 1881a(d)(e) and with the Fourth Amendment.").[3] Section 702 limits surveillance only to non-U.S. persons reasonably believed to be located outside the United States. 50 U.S.C. § 1881a(b). A significant purpose of the acquisition must be to obtain foreign intelligence information. 50 U.S.C. § 1881a(g)(2)(A)(5).

[3] Although [Caption Redacted] ultimately found the targeting and minimization procedures related to multi-communication transactions unreasonable under the Fourth Amendment, 2011 WL 10945618, at *28, the unconstitutional procedures were submitted to the FISC in April 2011, well after defendant was arrested.

The FISA Court of Review concluded the PAA's pre-surveillance procedures were sufficient to satisfy Fourth Amendment concerns. In re Directives, 551 F.3d at 1013. I am aware the PAA's incorporation of Executive Order 12333 included a requirement that surveillance targeting U.S. persons reasonably believed to be outside the United States had to be based on a finding by the Attorney General of probable cause to believe the target was a foreign power or agent of a foreign power. Section 702 has no such probable cause requirement. Section 702, however, prohibits targeting a U.S. person under any circumstances, even if the person is located outside the United States and acting as a foreign power or agent of a foreign power. Consequently, I conclude this difference does not diminish the particularity to the point of making the collections unreasonable under the Fourth Amendment.

The warrant and an inventory of seized property are returned to the issuing judge under Rule 41, and there are provisions to convey this information to the person whose property was seized. Defendant observes there are no similar provisions for a § 702 seizure. He argues the lack of notice and accountability under § 702 mean the person is never notified of the seizure, the searchers get no guidance on the limits of what can be read, and there is no process by which the FISC can know if the search and seizure were within the scope of the authorization.

The same notice provisions under 50 U.S.C. § 1806(c) cover FISA Title I/III, under which courts have long held surveillance is constitutional, and § 702. Importantly, defendant has now had full notice, giving him the ability to challenge the search and seizure. Minimization procedures, discussed in more detail below, provide guidance about what can be read. The FAA has oversight provisions requiring the Attorney General and DNI to regularly report compliance with targeting and

minimization procedures, as well as other data, to the FISC and congressional intelligence and judiciary committees. 50 U.S.C. § 1881a(l).

In sum, I do not find the lack of procedures associated with warrants make § 702 searches unreasonable under the Fourth Amendment.

c. Balancing the Governmental Interests Against the Intrusion on Privacy

I will now turn to balancing the legitimate governmental interests against the intrusion on an individual's privacy.

It is undisputed the government's interest in protecting the national security is compelling. "It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." Haig v. Agee, 453 U.S. 280, 307, 101 S. Ct. 2766 (1981) (internal quotation omitted) (the President has authority to revoke a passport because the person's activities in foreign countries are causing or are likely to cause serious damage to the national security or foreign policy of the United States). "[T]he Government's interest in combating terrorism is an urgent objective of the highest order." Holder v. Humanitarian Law Project, 561 U.S. 1, 28, 130 S. Ct. 2705 (2010) (analyzing statute criminalizing providing material support to foreign terrorist organization).

Defendant points to the statutory definition of foreign intelligence information to argue the government interest is too broadly defined, and thus intrudes on individual privacy too much, to justify the mass acquisition of Americans' electronic communications. The statute states:

> (e) "Foreign intelligence information" means–
>
> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e).

The FISA Court of Review describes subsection (2) as "information referred to as 'affirmative' or 'positive' foreign intelligence information rather than . . . 'protective' or 'counterintelligence' information. In re Sealed Case, 310 F.3d at 723, n.9. Defendant is concerned the government could interpret the "conduct of the foreign affairs of the United States" broadly enough to cover such items as international trade, rather than just threats to national security.

I note the discovery in this case all concerned protecting the country from a terrorist threat and did not stray into the broader category of the conduct of foreign affairs. I discuss this further in the classified opinion.

Under § 702, the intrusion of an individual's privacy is due to the incidental collection of the individual's communications during the acquisition of the communications from a targeted non-U.S. person reasonably believed to be outside the United States.[4] The government contends U.S. persons have limited expectations of privacy when communicating electronically with non-U.S. persons outside the United States. The government reasons the U.S. person assumes the risk that the foreign

[4] Defendant does not argue he was mistakenly targeted.

recipient will give the information to others, leave it freely accessible to others, or that the U.S. or foreign government will obtain the information.

The Fourth Amendment does not prohibit the government from obtaining information a person revealed to a third party, even if revealed in confidence. United States v. Miller, 425 U.S. 435, 444,96 S. Ct. 1619 (1976) (bank records). This concept also applies to electronic communications. "A person's reasonable expectation of privacy may be diminished in transmissions over the Internet or e-mail that have already arrived at the recipient." United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (internal quotation omitted).

Defendant offers the government cannot seize these communications without the consent of the recipient, which is an argument in favor of only the recipient's expectation of privacy in the communication. The sender's expectation of privacy has still been diminished.

Defendant also claims the minimization procedures for § 702 surveillance, as defined in 50 U.S.C. § 1801(h), provide no meaningful protection because the exclusions from the minimization procedures swallow the rule. As a result, the illusory minimization procedures make § 702 search and seizures unreasonable under the Fourth Amendment.

As I explain next, I conclude the minimization procedures contribute to the reasonableness of § 702 under the Fourth Amendment.

The government refers to a recently declassified document to support the reasonableness of § 702 minimization procedures.[5] The government also notes the FISC has repeatedly found

[5] Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (dated October 31, 2011), available at http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

materially equivalent minimization procedures sufficient in the context of traditional FISA electronic surveillance and physical search. Because these searches target U.S. persons in the United States, they are more likely to capture communications of non-targeted U.S. persons than the foreign communications captured under § 702. The government additionally relies on the FAA's oversight provisions requiring regular reports to the FISC and congressional oversight committees on the implementation of minimization procedures and the FISC's Rule of Procedure 13(b) which requires the government to report all instances of non-compliance.

The FISC has concluded the § 702 minimization procedures are consistent with the Fourth Amendment. [Caption Redacted], 2011 WL 10945618, at *6. In finding the PAA constitutional, the FISA Court of Review commented:

> It is also significant that effective minimization procedures are in place. These procedures serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons. The minimization procedures implemented here are almost identical to those used under FISA [Title I/III] to ensure the curtailment of both mistaken and incidental acquisitions.

In re Directives, 551 F.3d at 1015.

Section 6 of the declassified minimization procedures discusses the retention and dissemination of foreign communications of or concerning United States persons, putting limits on both. For example, the identity of the United States person is deleted in any dissemination of the information unless certain requirements are met. I do not agree with defendant that the minimization procedures provide no meaningful protection. On the contrary, I agree with the FISC that the minimization procedures contribute to the reasonableness of § 702 under the Fourth Amendment.

d. Querying After Acquisition

I now turn to defendant's most persuasive argument. He argues that even if § 702 warrantless surveillance is lawful, subsequent querying of the information after acquisition is a search requiring a warrant under the Fourth Amendment. Defendant draws analogies to United States v. Sedaghaty, 728 F.3d 885, 910-13 (9th Cir. 2013) (in a computer search authorized by warrant, the court rejected expansion of the warrant's expressly limited scope of items to be seized to include evidence related to background information providing a motive for the alleged crimes and stated in the affidavit supporting the warrant), United States v. Mulder, 808 F.2d 1346, 1348 (9th Cir. 1987) (pills lawfully in government possession could have been field tested for illegal drugs under a limited warrant exception, but laboratory testing to determine precise molecular structure required a warrant), and United States v. Young, 573 F.3d 711, 720-21 (9th Cir. 2009) (warrant required to search contents of a backpack taken by hotel security without evicting guest, and then given to police).

The government strongly disagrees. It distinguishes defendant's cases as analyzing government action beyond the scope of the warrant (or warrant exception). I agree with this characterization. Sedaghaty analyzed seizing evidence quite dissimilar from the items the warrant stated in its expressly limited list; Mulder and Young discussed whether to expand the private search warrant exception, as explained in United States v. Jacobsen, 466 U.S. 109, 104 S. Ct. 1652 (1984). As a result, I cannot draw analogies from these cases to support defendant's arguments.

Unfortunately, I do not find much assistance in most of the government's analogies either. Law enforcement computer queries of license plates and driver's licenses take place in a highly regulated arena and, in the case of license plates, are based on information displayed for all to see.

United States v. Diaz-Castaneda, 494 F.3d 1146, 1151-53 (9th Cir. 2007) (no reasonable expectation of privacy in a license plate so querying government databases about it is not a Fourth Amendment search; police can ask for identification of people who are legitimately stopped without performing a Fourth Amendment search). DNA profiles retained in a database to allow later law enforcement searches are from people who have been arrested or convicted. Boroian v. Mueller, 616 F.3d 60, 67-68 (1st Cir. 2010) ("government's retention and matching of [former probationer's] profile against [a DNA database] does not violate an expectation of privacy that society is prepared to recognize as reasonable, and thus does not constitute a separate search under the Fourth Amendment"). Neither of these limited invasions of privacy can be compared to the incidental acquisition of communications of U.S. persons.

The government also draws an analogy to minimization procedures under the Federal Wiretap Act which allow the government to use evidence from a wiretap to prove a crime unrelated to the original purpose for the wiretap. This analogy is more helpful because it addresses the use of communications obtained incidentally to those acquired by the wiretap. Specifically:

> When an authorized wiretap intercepts communications relating to offenses other than those specified in the order of authorization, 18 U.S.C. § 2517(5), disclosure or use of those communications is permissible provided a subsequent application . . . made to a judge of competent jurisdiction [demonstrates] the good faith of the original application. Such subsequent application would include a showing that the original order was lawfully obtained, that it was sought in good faith and not as a subterfuge search, and that the communication was in fact incidentally intercepted during the course of a lawfully executed order.

United States v. Goffer, 721 F.3d 113, 122-23 (2nd Cir. 2013) (internal quotations and citations omitted), pet. for cert. filed, No. 13-9973 13A777 (Apr. 2, 2014).

Because the government complied with all § 702 procedures concerning targeting and minimization, the government contends its actions were within the scope of the relevant legal authority and are thus distinguishable from defendant's cases. In its view, subsequent queries of information lawfully obtained, which do not implicate any reasonable expectation of privacy beyond that implicated in the initial lawful collection, do not constitute separate searches under the Fourth Amendment. The government claims this is true even if U.S. person identifiers are used in the querying.

The government notes the minimization procedures compel it to review information lawfully collected under § 702, which includes information about U.S. persons, to determine if the information should be retained or disseminated. According to the government:

> It would be perverse to authorize the unrestricted review of lawfully collected information but then to restrict the targeted review of the same information in response to tailored queries. Querying lawfully collected information using U.S.-person identifiers does not involve a significant additional intrusion on a person's privacy, beyond the level of intrusion already occasioned by the government as it reviews and uses information it lawfully collects under Section 702 pursuant to its need to analyze whether the information should be retained or disseminated.

Govt.'s Brief 57-58.

In the government's view, it must conduct such queries to fulfill its compelling interest to detect and disrupt terrorist attacks by discovering potential links between foreign terrorist groups and people within the United States.

It is true, the FISC has approved minimization procedures which allow querying using U.S. person identifiers. [Caption Redacted], 2011 WL 10945618, at *8. While the procedures previously imposed a "wholesale bar" on such queries, the new approved procedures allowed queries with U.S. person identifiers "subject to approval pursuant to internal NSA procedures and oversight by the

Department of Justice." Id. The FISC reasoned it had approved FISA Title I applications targeting U.S. persons that used minimization procedures allowing queries with U.S. person identifiers.

> It follows that the substantially-similar querying provision found at Section 3(b)(5) of the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons.

Id.

This is a very close question. On the one hand, why not require a warrant when using a U.S. person identifier to search a database of information already gathered? That is not the test, however–just because a practice might better protect Americans' privacy rights does not mean the Fourth Amendment requires the practice. Indeed, as the government argues, it must review information lawfully collected to decide whether to retain or disseminate it under the minimization procedures. As the FISC reasoned, the § 702 collection, by being aimed at non-U.S. persons believed to be outside the United States, is less likely to acquire information about non-consenting U.S. persons than a FISA Title I collection. I do not find any significant additional intrusion past what must be done to apply minimization procedures. Thus, subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment.

e. Summary

To sum up, I must examine the totality of the circumstances and weigh the government's compelling interest in protecting national security against the degree to which § 702 surveillance intrudes on an individual's privacy. See Samson, 547 U.S. at 848; King, 133 S. Ct. at 1970.

Section 702 has numerous safeguards built into the statute. Most importantly, § 702 is aimed at acquiring foreign intelligence information in electronic communications from non-U.S. persons located outside the United States. There are additional limitations, including that the statute cannot "intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States[.]" 50 U.S.C. § 1881a(b)(2). Minimization procedures protect the privacy of U.S. persons whose communications are incidentally acquired. The Attorney General and DNI must certify, among other things, that appropriate targeting and minimization procedures are in place and a significant purpose of the acquisition is to obtain foreign intelligence information. 50 U.S.C. § 1881a(g)(2)(A). The FISC must find the targeting and minimization procedures consistent with the Fourth Amendment. Congress and the FISC provide oversight based on specific reporting requirements.

Based on the statutory protections, I conclude the government's compelling interest in protecting national security outweighs the intrusion of § 702 surveillance on an individual's privacy. Accordingly, § 702, as applied to defendant, is reasonable under the Fourth Amendment.

E. Acquisition of Section 702 Materials in this Case

Even if the court concludes § 702 is constitutional, defendant correctly notes that any acquisition, retention, accessing, dissemination, and use of the seized electronic communications which exceed the FISC authorizations are unlawful. Defendant's concerns are heightened by declassified FISC opinions indicating that some § 702 surveillance might have exceeded the authorizations. Defendant asks the court to obtain extensive background material to assure the

surveillance was lawfully conducted under the statute and, if not, to suppress all evidence derived from it.

The government contends once I perform an in camera, ex parte review of the relevant classified materials, I will conclude the § 702 acquisition was lawfully authorized and conducted.

I made a careful de novo, ex parte review of the § 702 applications and conclude the certification required by 50 U.S.C. § 1881a(g)(2)(A) was in place. I also find that the government agents followed appropriate targeting and minimization procedures. Thus, I conclude the § 702 surveillance at issue here was lawfully conducted.

F. Suppression Based on Other Alleged Surveillance Activities

Defendant raises concerns about the collection of telephone metadata under § 215 of the Patriot Act, codified at 50 U.S.C. § 1861, and any other still-secret warrantless surveillance programs. He assumes there is a strong possibility that his telephone metadata has been collected, and he asks the court to address the lawfulness of these programs, conclude they violate the First and Fourth Amendments, and suppress all fruits of these other surveillance activities.

I deny defendant's arguments concerning § 215 for the reasons stated in the classified opinion.

G. Good Faith Exception

As an alternative argument, the government claims the good faith exception to the exclusionary rule, as set forth in United States v. Leon, 468 U.S. 897 (1984), provides an independent basis for denying defendant's suppression motion. The government argues the exception applies here because the § 702 collection was authorized by a duly-enacted statute, law

enforcement officers reasonably relied on orders of a neutral magistrate, namely the judges of the FISC, and the FISA Court of Review has upheld similar directives issued under the PAA.

Defendant contends the court should not attach a good faith exception to FISA because the statute, which preceded Leon, does not contain an exception in its statutory suppression provision, 50 U.S.C. § 1806(g). Defendant distinguishes the government's other cases because they address situations where officers relied on an individualized FISA or other judicial order, which was not done here. See United States v. Ning Wen, 477 F.3d 896, 897-98 (7th Cir. 2007) (FISA warrant). Defendant further claims the government knew of the constitutional objections from the day of enactment of the FAA due to the immediate initiation of litigation in Clapper.

I will first address defendant's last argument concerning the initiation of litigation against § 702. I see no reason for the government to assume all challenges to a statute will be successful; numerous warrants issued under FISA Title I/III have survived challenges. A statute is constitutional until a court declares otherwise. Moreover, even the defendant who succeeds in having a statute declared unconstitutional is not guaranteed application of the exclusionary rule. See Duka, 671 F.3d at 346 (quoted below).

Under the good faith exception to the exclusionary rule established in Leon, the government has the burden of demonstrating the officer acted "'in objectively reasonable reliance' on the warrant." United States v. Underwood, 725 F.3d 1076, 1085 (9th Cir. 2013) (quoting Leon, 468 U.S. at 922)).[6] "Exclusion is not a personal constitutional right, nor is it designed to redress the

[6] There are four situations that per se fail to satisfy the good faith exception, as explained in Underwood, but they do not fit well into the issue before me because the situations assume the exception is being applied to a warrant.

In these situations, "the officer will have no reasonable grounds for believing that

injury occasioned by an unconstitutional search." Davis v. United States, 131 S. Ct. 2419, 2426 (2011) (internal quotations omitted) (refusing to apply exclusionary rule when police conduct a search in objectively reasonable reliance on binding appellate precedent). Even if a court finds the statute on which a warrant is based unconstitutional, the evidence is not automatically suppressed:

> The Supreme Court has ruled categorically that "suppress[ing] evidence obtained by an officer acting in objectively reasonable reliance on a statute" would not further the purposes of the exclusionary rule, even if that statute is later declared unconstitutional. Illinois v. Krull, 480 U.S. 340, 349–50, 107 S. Ct. 1160, 94 L. Ed. 2d 364 (1987). Therefore, even a defendant who can establish that evidence against him or her was procured under a statute that violates the Fourth Amendment is not entitled to have such evidence excluded from his or her criminal trial unless he or she can establish that the officer's reliance on the statute was not objectively reasonable.

Duka, 671 F.3d at 346 (after finding FISA's amended "significant purpose" test was reasonable under the Fourth Amendment, the Third Circuit alternatively held it would not apply the exclusionary rule to evidence obtained under a FISA *warrant*, even if it had held FISA was unconstitutional).

Defendant's argument, based on the fact that there is no exception in FISA's statutory exclusion provision, draws an analogy to wiretaps under Title III. Some courts have held the good faith exception to the warrant requirement does not apply to wiretap warrants under Title III. United States v. Rice, 478 F.3d 704, 711 (6th Cir. 2007) ("the language in Title III provides that exclusion is

---

> the warrant was properly issued." 468 U.S. at 922–23, 104 S. Ct. 3405. The four situations are: (1) where the affiant recklessly or knowingly placed false information in the affidavit that misled the issuing judge; (2) where the judge "wholly abandon[s] his [or her] judicial role"; (3) where the affidavit is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) where the warrant is "so facially deficient–i.e., in failing to particularize the place to be searched or the things to be seized–that the executing officers cannot reasonably presume it to be valid." Id.

Underwood, 725 F.3d at 1085.

the exclusive remedy for an illegally obtained warrant. In contrast to the law governing probable cause under the Fourth Amendment, the law governing electronic surveillance via wiretap is codified in a comprehensive statutory scheme providing explicit requirements, procedures, and protections."). Other courts have held the opposite. United States v. Moore, 41 F.3d 370, 376 (8th Cir. 1994) (good faith exception can apply to warrants under Title III); United States v. Malekzadeh, 855 F.2d 1492, 1497 (11th Cir.1988) (same). The Ninth Circuit has not expressly analyzed application of the good faith exception to evidence obtained pursuant to a Title III wiretap. See United States v. Duran, 189 F.3d 1071, 1084-87 (9th Cir. 1999) (court did not exclude wiretap evidence after concluding Title III preconditions to judicial authorization of wiretap were satisfied even though the application did not cover the possibility the target might purchase a new cell phone; court did not address government's proffered good faith exception). Defendant asks me to apply the Sixth Circuit holding to § 702.

With the split in the circuits and no Ninth Circuit precedent, little is to be gained from analogizing § 702 to Title III wiretaps. I will proceed instead to the policy reasons behind the exclusionary rule. I also must examine the policy reasons because there is no traditional warrant under § 702. That was the case in Krull, in which the Court expanded the Leon good faith exception and did not exclude evidence obtained by police acting in objectively reasonable reliance on a state vehicle code authorizing warrantless administrative searches, even though a court later held the statute violated the Fourth Amendment. Krull, 480 U.S. at 349-50, 356-57. The Court reasoned the prime purpose of the exclusionary rule was to "deter future unlawful police conduct"; it was not meant to punish judges or magistrates. Id. at 347, 348. In extending the good faith exception, the Court likened the role of a magistrate in issuing warrants to the role of a legislature in passing legislation:

> The approach used in Leon is equally applicable to the present case. The application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer's actions as would the exclusion of evidence when an officer acts in objectively reasonable reliance on a warrant. Unless a statute is clearly unconstitutional, an officer cannot be expected to question the judgment of the legislature that passed the law. If the statute is subsequently declared unconstitutional, excluding evidence obtained pursuant to it prior to such a judicial declaration will not deter future Fourth Amendment violations by an officer who has simply fulfilled his responsibility to enforce the statute as written.

Id. at 349.

Addressing an argument that applies equally well to § 702 surveillance, the Court was also unpersuaded by the fact that a "statute authorizing warrantless administrative searches affects an entire industry and a large number of citizens, while the issuance of a defective warrant affects only one person." Id. at 350.

> Real deterrent value is a "necessary condition for exclusion," but it is not "a sufficient" one. Hudson v. Michigan, 547 U.S. 586, 596, 126 S. Ct. 2159, 165 L. Ed. 2d 56 (2006). The analysis must also account for the "substantial social costs" generated by the rule. Leon, supra, at 907, 104 S. Ct. 3405. Exclusion exacts a heavy toll on both the judicial system and society at large. Stone, 428 U.S., at 490–491, 96 S. Ct. 3037. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. Ibid. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. See Herring, supra, at 141, 129 S. Ct. 695. Our cases hold that society must swallow this bitter pill when necessary, but only as a "last resort." Hudson, supra, at 591, 126 S. Ct. 2159. For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs. See Herring, supra, at 141, 129 S. Ct. 695; Leon, supra, at 910, 104 S. Ct. 3405.

Davis, 131 S. Ct. at 2427.

Here, the § 702 surveillance was based on a statute Congress enacted and a certification the FISC approved. Law enforcement was only acting based on the FISC's approval. The judicial approval makes law enforcement's reliance more objectively reasonable than the officer's reliance in

Krull, in which the administrative search took place under a statute that required no judicial approval of the programs based on it. Even if I found § 702 unconstitutional, exclusion of the evidence here would not deter unconstitutional actions by law enforcement. For these reasons, I conclude the good faith exception should apply.

H. Request for Franks Hearing

Defendant seeks a hearing under Franks v. Delaware, 438 U.S. 154 (1978), to challenge the validity of the representations made to the FISC to obtain the FISA warrants already considered by the court in this case.

In Franks, the Supreme Court held that, under certain circumstances, a defendant is entitled to an evidentiary hearing in which he can attack the veracity of a search warrant affidavit or challenge the omission of material facts in the affidavit. When a defendant seeks a Franks hearing because of "allegations of material false statements or omissions in an affidavit supporting a search warrant, a defendant must make a substantial preliminary showing that false or misleading statements were (1) deliberately or recklessly included in an affidavit submitted in support of a search warrant; and (2) necessary to the finding of probable cause." United States v. Flyer, 633 F.3d 911, 916 (9th Cir. 2011) (internal quotations omitted).

Defendant argues the existence of previously undisclosed surveillance under § 702 and telephone metadata collection programs raise serious questions on whether the government reported the entire story to the FISC in the applications. Defendant argues he is precluded from making the normal substantial preliminary showing to obtain a Franks hearing because the government and the court have refused to disclose the FISA warrant applications.

The government responds that defendant's lack of access to the FISA applications does not ease his burden to make a substantial preliminary showing of misrepresentations essential to the finding of probable cause or, in the case of § 702 surveillance, essential to support the certification from the Attorney General and DNI. Moreover, the government insists defendant's allegations about the government's lack of candor to the court in other federal cases involving national security issues cannot establish that any errors were made in this case.

I must agree with the government on the last point. If misrepresentations in one case were attributed to the government in unrelated cases, all defendants would be entitled to a Franks hearing without making the required preliminary showing.

Defendant's position has not changed since the pretrial FISA suppression motion–he can only speculate about false statements or omissions. This is insufficient to qualify as a substantial preliminary showing. I realize the difficult position the defense team is in, but the denial of a Franks hearing is commonplace in the FISA context and goes hand-in-hand with the ex parte judicial review process. See United States v. Abu-Jihaad, 630 F.3d 102, 130 (2nd Cir. 2010); United States v. el-Mezain, 664 F.3d 467, 570 (5th Cir. 2011); United States v. Damrah, 412 F.3d 618, 624-25 (6th Cir. 2005). Cf. United States v. Daoud, No. 14-1284, 2014 WL 2696734 (7th Cir. June 16, 2014) (Rovner, J., concurring) (explaining difficulties defendants face in getting a Franks hearing in the FISA context).

I. Renewed Motion for Discovery

Although FISA allows the court to make an in camera, ex parte review of materials when deciding a motion to suppress, the statute does allow the aggrieved person to receive discovery in certain circumstances. Specifically, "In making this determination, the court may disclose to the

aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f).

Defendant renews his motion for discovery so he may hone his arguments. He insists the court should interpret the term "necessary" in § 1806(f) to mean something closer to "helpful" or "appropriate" and not "absolutely necessary" or "essential."

I am aware of a single district court which granted defendant's motion for disclosure of FISA materials to defense counsel with security clearances. United States v. Daoud, No. 12-CR-723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014) (order stayed pending appeal). The government's only response to the motion was that disclosure had never been ordered. The court found the response inadequate to explain how national security would be harmed by disclosure to properly cleared defense counsel. Id. at *2. The Seventh Circuit just reversed the district court, however, holding the court cannot order disclosure of the classified materials without first finding that the "disclosure is necessary to make an accurate determination of the legality of the surveillance[,]" as provided in FISA. United States v. Daoud, 2014 WL 2696734. The Circuit further held that it was possible for the court to determine the legality of the investigation without disclosure of the classified materials to defense counsel, and that the investigation did not violate FISA. Id.

I am unconvinced by both defendant's arguments and the district court in Daoud–classified material is at issue here. The Ninth Circuit has rejected the argument that FISA materials can be turned over if defense counsel has the appropriate security clearances:

> Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question, whether or not she happens for unrelated reasons to enjoy security clearance. We reject the notion that a defendant's due process right to disclosure of FISA materials turns on the qualifications of his counsel.

United States v. Ott, 827 F.2d 473, 477 (9th Cir. 1987) (holding FISA's ex parte in camera proceedings do not violate due process, even though defense counsel had high security clearances).

"[D]isclosure of FISA materials is the exception and *ex parte, in camera* determination is the rule." Abu-Jihaad, 630 F.3d at 129 (internal quotation omitted); el-Mezain, 664 F.3d at 567 (same, quoting Abu-Jihaad). Obviously it would be helpful to the court to have defense counsel review the materials prior to making arguments. Congress, however, did not put "helpful" in the statute; it chose "necessary." I interpret "necessary" to be much closer to "essential" than to "helpful." And I do not find disclosure to the defense is necessary for me to make an accurate determination of the legality of the surveillance.

Moreover, in my review of the FISA materials associated with this motion and the previous FISA suppression motion, I have seen "no indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, or any other factors that would indicate a need for disclosure" here. Ott, 827 F.2d at 476 (internal quotation omitted).

Accordingly, I deny defendant's motion for discovery.

CONCLUSION

Defendant's Motion for Vacation of Conviction and Alternative Remedies of Dismissal of the Indictment, Suppression of Evidence, and New Trial for the Government's Violation of the

Pretrial Notice Statute [500], defendant's Alternative Motion for Suppression of Evidence and a New Trial Based on the Government's Introduction of Evidence at Trial and Other Uses of Information Derived from Unlawful Electronic Surveillance [502], and defendant's Second Motion for a New Trial [504] are denied.

IT IS SO ORDERED.

Dated this 24th day of June, 2014.

/s/ Garr M. King
Garr M. King
United States District Judge